Start of new case

Q1 Does the draft guidance cover the relevant issues about the right of access?

- [x] Yes
- [ ] No
- [ ] Unsure / don't know

If no or unsure/don’t know, what other issues would you like to be covered in it?

Q2 Does the draft guidance contain the right level of detail?

- ○ Yes
- ◉ No
- ○ Unsure / don't know

If no or unsure/don't know, in what areas should there be more detail within the draft guidance?

The part that remains unclear is establishing identity. The guidance says: "The level of checks you make may depend on the possible harm and distress that inappropriate disclosure of the information could cause to the individual concerned." This means, the greater the possible harm, the more stringent the identity checks need to be, right? In view of the increase in identity theft, shouldn't more stringent measures be applied across the board anyway? It would be helpful to have a chart with (please imagine the items side-by-side): "Such-and-such circumstances" then... "Use such-and-such method of establishing identity." So the top of the chart would be for example: "Internal SARs such as from employees, or well-known customers then... "Additional proof of identity would usually be superfluous" The end of the chart could be: "The customer's identity could not be confirmed by means of questions regarding e.g. their account details and the customer is not well-known or new, or any suspicious circumstances" then... "Strong proof of identity should be required. Acceptable proof of identification will be a selfie/photo of the person holding either their passport or their driving licence directly beneath their chin. The quality of the selfie must be such that the person's entire face as well as their passport photo can clearly be seen on the passport/driving license and that the person's name is legible. The person should block out their passport number and/or address as these are irrelevant and could pose an additional data burden. This is to prevent someone with unauthorised access to another person's passport/driving license from simply sending a copy of the document and thereby gaining access to additional personal data, such as could very likely happen in the case of attempted identity theft" To me, the disconcerting ease with which a SAR can be weaponized is alarming, and it's just a matter of time before professional cyber criminals cotton onto this and begin exploiting it.

Q3 Does the draft guidance contain enough examples?

- [x] Yes
- [ ] No
- [ ] Unsure / don't know

If no or unsure/don’t know, please provide any examples that think should be included in the draft guidance.

Q4 We have found that data protection professionals often struggle with applying and defining 'manifestly
unfounded or excessive' subject access requests. We would like to include a wide range of examples
from a variety of sectors to help you. Please provide some examples of manifestly unfounded and excessive
requests below (if applicable).

Q5 On a scale of 1-5 how useful is the draft guidance?

1 - Not at all useful	2 – Slightly useful	3 – Moderately useful	4 – Very useful	5 – Extremely useful
○	○	○	✓	○

Q6 Why have you given this score?

I found the guidance on identity verification somewhat inadequate; everything else was good.

Q7 To what extent do you agree that the draft guidance is clear and easy to understand?

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	✓

Q8 Please provide any further comments or suggestions you may have about the draft guidance.

To reiterate: The disconcerting ease with which a SAR can be weaponized is alarming, and it's just a matter of time before professional cyber criminals cotton onto this and begin exploiting it en masse. Stronger identity verification needs to be in place to prevent this.

Q9 Are you answering as:

- ○ An individual acting in a private capacity (eg someone providing their views as a member of the public)
- ◉ An individual acting in a professional capacity
- ○ On behalf of an organisation
- ○ Other

Please specify the name of your organisation:

Venom IT

Q10 How did you find out about this survey?

- ○ ICO Twitter account
- ○ ICO Facebook account
- ○ ICO LinkedIn account
- ○ ICO website
- ◉ ICO newsletter
- ○ ICO staff member
- ○ Colleague
- ○ Personal/work Twitter account
- ○ Personal/work Facebook account
- ○ Personal/work LinkedIn account
- ○ Other

Thank you for taking the time to complete the survey